



Issuance of Indonesia's New Implementing Regulation on Personal Data Protection

September 2026

One Asia Lawyers Indonesia Office

Japanese Lawyer Koji Umai

Indonesian Lawyer Prisilia Sitompul

Indonesian Lawyer Kevin Anggiat Harahap

1. Introduction

On 16 July 2026, the Government of Indonesia promulgated Government Regulation No. 33 of 2026 on the Implementation of Law No. 27 of 2022 on Personal Data Protection ("**GR 33/2026**"). GR 33/2026 provides that it will take effect six months after its promulgation, on 16 January 2027.



GR 33/2026 was enacted as the implementing regulation of Law No. 27 of 2022 on Personal Data Protection (the "**PDP Law**").

The PDP Law entered into force on 17 October 2022, with a two-year transition period that expired on 17 October 2024 (Article 74 of the PDP Law). However, the PDP Law provided that many matters would be further regulated by Government Regulation, leaving a number of details to be addressed. GR 33/2026 sets out the content and implementation of obligations under the PDP Law in greater detail.

2. Key Additions and Clarifications under GR 33/2026

a. Lawful Bases for Processing

Article 20 of the PDP Law requires a Personal Data Controller to have one of the following lawful bases when processing personal data: (i) explicit consent from the data subject; (ii) performance of contractual obligations; (iii) compliance with legal obligations; (iv) protection of the data subject's vital interests; (v) performance of a task in the public interest or exercise of public authority; or (vi) other legitimate interests.

The draft implementing regulation published in 2023 set out more detailed requirements for relying on each of these lawful bases.¹ GR 33/2026 largely follows this basic framework. For example, it requires consent to be freely given, informed, specific and unambiguous, and prohibits obtaining consent by deceptive or misleading means. It also prohibits refusing to provide goods or services, or reducing their quality, solely because the data subject has not consented, unless the processing of personal data is necessary for the provision of those goods or services (Articles 32 to 39).

With respect to performance of contractual obligations, GR 33/2026 provides that personal data may be processed where necessary to perform contractual obligations under a contract to which the data subject is a party, or where necessary to take steps at the request of the data subject before entering into a contract. It also sets out further details, including the minimum

¹ See also the following newsletters regarding the draft implementing regulation:

Towards the Issuance of the Implementing Regulation under Indonesia's Personal Data Protection Law (1)

<https://oneasia.legal/11565>

Towards the Issuance of the Implementing Regulation under Indonesia's Personal Data Protection Law (2) — Cross-Border Transfers

<https://oneasia.legal/11768>

Towards the Implementation of the Implementing Regulation under Indonesia's Personal Data Protection Law (3) — Personal Data Processing

<https://oneasia.legal/13885>



matters to be included in a contract relied upon as the basis for processing, the conditions applicable to requests made by a data subject before entering into a contract, and the cessation of processing (Articles 40 to 44).

Where other legitimate interests are relied upon as the basis for processing, GR 33/2026 requires an analysis and assessment of the purpose and necessity of the processing, the balance between the controller's interests and the rights of the data subject, any potential legal effects or adverse impact on the data subject, and the relevant mitigation measures, with the results to be documented (Articles 53 to 57).

The basic framework under GR 33/2026 concerning these lawful bases does not differ substantially from the 2023 draft implementing regulation, although certain provisions have been revised.

Of particular note is the treatment of performance of contractual obligations as a lawful basis. The 2023 draft implementing regulation contained a provision requiring explicit and valid consent from the data subject for contracts involving personal data processing, which left the relationship between contract as an independent lawful basis and consent somewhat unclear.

By contrast, GR 33/2026 more clearly treats performance of contractual obligations as a lawful basis that is independent from consent.

b. Provision of Information

Article 21 of the PDP Law prescribed the information to be provided where consent is relied upon as the lawful basis, but did not expressly state that the same notification obligation applies to all other lawful bases. Article 62 of GR 33/2026 now requires the prescribed information to be provided, in principle before processing begins, regardless of the lawful basis relied upon. Where personal data is obtained indirectly rather than directly from the data subject, the Personal Data Controller must provide the above information to the data subject within 30 business days after obtaining the data (Article 64).

In addition, where consent is obtained for the purpose of offering or introducing goods or services, GR 33/2026 requires clear information to be provided concerning, among other matters, the third parties that will receive the personal data, the form in which the goods or services will be offered or introduced, and the method for withdrawing consent (Article 35(2)). The elucidation to that Article states that the relevant "third-party information" includes information identifying the third party, the purpose for which the data will be received, and the types of personal data to be received. Although the 2023 draft implementing regulation already required information concerning third parties to be provided, GR 33/2026 newly clarifies the specific content of that information, which may affect future practices for obtaining consent in connection with the offering or introduction of goods or services.

c. Governance and Accountability

The PDP Law provides for records of processing activities (Article 31 of the PDP Law), data protection impact assessments ("DPIA") for high-risk personal data processing (Article 34 of the PDP Law), a personal data protection officer ("DPO") (Articles 53 and 54 of the PDP Law), and basic obligations concerning joint controllers and processors (Article 18 of the PDP Law). The PDP Law also requires notification to data subjects in connection with transfers of personal data arising from mergers and similar corporate actions (Article 48 of the PDP Law).

In this regard, Article 74 of GR 33/2026 requires Personal Data Controllers to prepare and maintain records of processing activities, including an inventory and mapping of data flows, processing purposes and legal bases, categories of personal data and data subjects, retention periods, security measures and cross-border transfers. It also specifies matters to be included in agreements and other arrangements with joint controllers and processors, and requires written arrangements with sub-processors to ensure an equivalent level of personal data protection.



GR 33/2026 also clarifies that a DPIA must be conducted before high-risk personal data processing begins and provides further detail on the matters to be assessed and the review of the DPIA (Articles 120 to 122). With respect to the DPO, the Regulation establishes organisational requirements intended to ensure the effectiveness of the role, including a reporting line to the highest level of management, independent performance of duties, adequate resources and access to processing activities, and avoidance of conflicts of interest (Articles 142 to 147).

The Regulation further provides more detailed procedures for personal data transfers in connection with mergers and similar corporate actions, including pre-transfer assessments, the contents of notifications and the exercise of data-subject rights (Articles 131 to 137). In particular, a new Personal Data Controller may not process the transferred personal data for its own purposes until the period for objections by data subjects has expired (Article 135(2)).

d. Cross-Border Transfers of Personal Data

For multinational companies, the provisions on cross-border transfers are among the particularly important matters under GR 33/2026. The basic framework is already set out in Article 56 of the PDP Law, which establishes the following sequential requirements for cross-border transfers:

- (a). the level of personal data protection in the receiving country is equivalent to or higher than the level of personal data protection in Indonesia;
- (b). if item (a) is not satisfied, adequate and binding personal data protection safeguards are ensured in the receiving country; or
- (c). if neither item (a) nor item (b) is satisfied, the data subject's consent to the transfer is obtained.

The PDP Law provided that further details concerning these requirements would be stipulated in the implementing regulation (Article 56(5) of the PDP Law).

GR 33/2026 requires Personal Data Controllers to conduct a risk assessment for cross-border transfers and, in advance, to provide data subjects with information concerning matters including the purpose of the transfer, the measures used to protect personal data, the method for exercising rights, and the risks associated with the transfer and the relevant mitigation measures (Article 164(1) and (2)). Because Article 164 establishes this information obligation separately from the transfer requirements set out in Article 165, it is considered that, in principle, such information must also be provided where the receiving country has an equivalent or higher level of protection or where the transfer is made on the basis of adequate and binding safeguards.

The Regulation also sets out criteria for adequacy assessments by the competent authority and requires the authority to establish a list of jurisdictions or international organisations that provide an equivalent or higher level of protection (Article 168).

In addition, GR 33/2026 recognises standard contractual clauses, binding corporate rules (BCR) and other recognised instruments as mechanisms that may constitute adequate and binding safeguards (Article 169).

The Regulation further makes clear that consent is not an unrestricted alternative mechanism, and imposes requirements including that the transfer is non-repetitive, involves a limited number of data subjects, and is supported by an appropriate risk assessment and safeguards (Article 173).

Further details concerning these requirements are to be regulated by rules of the competent authority, and future regulatory developments should therefore continue to be monitored (Articles 168(4), 172 and 174).

e. Data Breach Response and Enforcement



The PDP Law provides that, where a personal data protection incident occurs, written notification must be provided to the data subject and the competent authority within 3 × 24 hours (Article 46 of the PDP Law).

GR 33/2026 does not change this deadline, but clarifies that the period begins when the occurrence of the data breach is known with sufficient certainty and reasonableness (Article 114(2)). It also requires Personal Data Controllers to establish internal policies and procedures for incident prevention and response, including the allocation of responsibilities, incident analysis and prioritisation, reporting, recordkeeping and periodic review (Article 117). A Personal Data Processor must report a relevant incident to the Personal Data Controller as soon as possible (Article 118).

With respect to administrative sanctions, Article 57 of the PDP Law provides for written warnings, temporary suspension of processing activities, deletion or destruction of personal data, and administrative fines of up to 2% of annual revenue or annual receipts. GR 33/2026 further specifies the enforcement framework by identifying the provisions subject to administrative sanctions, the factors and variables to be considered in imposing sanctions and calculating fines, and the procedures for investigation, decision and objection (Articles 184 to 199). It also permits multiple administrative sanctions to be imposed simultaneously and does not require a written warning to be imposed before another sanction (Article 184(7) and (8)).

3. Practical Measures for Businesses

The implementation of GR 33/2026 does not mean that companies need to rebuild their existing PDP Law compliance framework from scratch. Rather, companies should review the PDP Law compliance measures already in place in light of the requirements clarified or added by GR 33/2026 and take any additional measures that may be necessary.

In doing so, it is important to retain the necessary records and supporting materials so that, if a personal data protection issue arises, the company can reasonably explain and demonstrate that its governance framework and response were appropriate.

In particular, companies may consider taking the following steps in preparation for the Regulation taking effect on 16 January 2027:

- Review of lawful bases and information provision: Reconfirm the lawful basis for each processing activity, prepare the necessary documentation such as legitimate-interest assessments, and confirm that privacy notices and consent mechanisms satisfy the information requirements under GR 33/2026.
- Strengthening data-processing governance: Prepare and update records of processing activities, review agreements with joint controllers, processors, vendors and other relevant parties, and confirm that governance arrangements, including DPIAs and the DPO function, satisfy the requirements of GR 33/2026.
- Cross-border transfer compliance: Map cross-border data flows, confirm the applicable transfer mechanism and any necessary risk assessments and safeguards for each transfer, and review the information provided to data subjects in relation to cross-border transfers.
- Personal data protection incidents: Establish internal policies and procedures for the prevention of and response to personal data breaches.
- Corporate reorganisations and transactions: Review notifications, objection-handling procedures and other required steps for transfers of personal data in connection with mergers, acquisitions, spin-offs and similar transactions.

Based on the above, companies are also recommended to update internal privacy policies, privacy notices, consent forms and Data Processing Agreements, and to make the necessary preparations for responding to personal data breaches.

4. Conclusion



As described above, GR 33/2026 does not alter the basic personal data protection framework established under the PDP Law, but further specifies the procedures and requirements necessary for its implementation. As a result, Indonesia's personal data protection regime is expected to move into a more practical stage of implementation.

Accordingly, companies operating in Indonesia should review the specific requirements under GR 33/2026, including the matters discussed in this newsletter, and take any additional measures that may be necessary.

GR 33/2026 also leaves a number of matters to be further regulated by rules of the competent personal data protection authority. Companies should therefore continue to monitor future subordinate regulations while proceeding with preparations for the Regulation taking effect on 16 January 2027.

◆ One Asia Lawyers ◆

One Asia Lawyers Group is a network of independent law firms established to provide seamless and comprehensive legal advice to Japanese clients operating across Asia. One Asia Lawyers Group has member firms in Japan, ASEAN, South Asia and Oceania, and is composed of legal specialists in each jurisdiction, providing practical and seamless legal services rooted in each region.

For inquiries regarding this article, please visit <https://oneasia.legal> or contact us at info@oneasia.legal.

This newsletter is intended to provide general information only and does not constitute legal advice of the Group or its member firms. Any views expressed are the personal views of the authors and do not represent the views of the Group or its member firms. Given the general informational nature of this newsletter, citations to statutory provisions and sources may in some cases be intentionally omitted. For advice on specific matters, please consult the relevant member firm or lawyer.

<Authors>

	Koji Umai Representative, One Asia Lawyers Indonesia Office Japanese Lawyer Koji worked at a law firm in Japan for six years, handling a wide range of corporate legal matters, while also gaining experience in international matters involving general civil law, family and inheritance law, insolvency and criminal law. After studying Asian business and financial law at Singapore Management University in 2018, he joined One Asia in 2020. He currently advises on market-entry strategies in light of the latest regulatory and legislative developments, ongoing legal support, contracts, employment matters, general corporate legal affairs, compliance and dispute response. koji.umai@oneasia.legal
	Prisilia Sitompul One Asia Lawyers Indonesia Office Indonesian Lawyer Prisilia worked for more than six years as in-house counsel in the legal department of an Indonesian energy and natural resources company, where she handled a variety of legal matters relating to the energy and natural resources sector. She holds a master's degree from the University of Aberdeen in the United Kingdom, specialising in Oil and Gas Law. After joining the Tokyo office of One Asia Lawyers, she has provided various forms of legal support as an Indonesian lawyer, including Indonesian-law research and contract review for Japanese companies operating in Indonesia. She also assists Indonesian companies investing in Japan. sitompul.prisilia@oneasia.legal
	Kevin Anggiat Harahap One Asia Lawyers Indonesia Office Indonesian Lawyer Kevin is an Indonesian-qualified lawyer who advises Japanese companies on a broad range of matters relating to their business operations in Indonesia. His



practice covers corporate establishment and foreign investment, M&A and corporate restructuring, commercial transactions and contracts, regulatory matters, as well as dispute-related matters.

Prior to joining One Asia Lawyers, Kevin worked at law firms in Indonesia and Tokyo, where he advised Japanese and multinational companies on Indonesian legal matters. Drawing on his practical experience in both Indonesia and Japan, he has extensive experience in cross-border transactions and a broad range of corporate and commercial matters.

Kevin holds an LL.B. from the University of Indonesia and an LL.M. from Keio University Law School. He is qualified to practice law in Indonesia through the Indonesian Advocates Association (PERADI).

kevin.harahap@oneasia.legal